CLAIMS

1. A method comprising:

establishing a secure communication channel between a media playback application and a component downstream from the media playback application; and

using the secure communication channel to at least enable the media playback application to instruct the downstream component to enable one or more of a number of different types of content protection technologies to protect media content that is provided over a physical connector.

2. The method of claim 1 further comprising using the secure communication channel to enable the media playback application to instruct the downstream component as to how to apply one or more of the different types of content protection technologies.

3. The method of claim 1, wherein the downstream component comprises a software component.

4. The method of claim 1 further comprising using the secure communication channel to enable the media playback application to request status information from the downstream component.

5. The method of claim 1 further comprising:

using the secure communication channel to enable the media playback application to request status information from the downstream component; and

using the secure communication channel to receive status information from the downstream component.

6. The method of claim 1 further comprising:

using the secure communication channel to enable the media playback application to request status information from the downstream component; and

using the secure communication channel to receive status information from the downstream component, wherein the status information pertains to instructions that were previously sent by the media playback application.

7. The method of claim 1 further comprising:

using the secure communication channel to enable the media playback application to request status information from the downstream component; and

using the secure communication channel to receive status information from the downstream component, wherein the status information does not pertain to instructions that were previously sent by the media playback application.

8. One or more computer-readable media having computer-readable instructions which, when executed, implement the method of claim 1.

9. A computing system embodying the one or more computer-readable media of claim 8.

10. A system comprising:

one or more computer-readable media;

a software component resident on the media and configured to:

establish a secure communication channel with a media playback application;

use the secure communication channel to receive instructions from the media playback application to enable one or more of a number of different types of content protection technologies to protect media content that is provided over a physical connector; and

for at least some of the content protection technologies, receive instructions to configure the content protection technologies.

11. The system of claim 10, wherein the software component comprises a software driver.

12. The system of claim 10, wherein the software component is further configured to use the secure communication channel to receive status requests from the media playback application.

13. The system of claim 10, wherein the software component is further configured to use the secure communication channel to receive status requests from the media playback application, and wherein the software component is further configured to use the secure communication channel to send status information to the media playback application.

14. The system of claim 10, wherein the software component is further configured to use the secure communication channel to receive status requests from the media playback application, and wherein the software component is further configured to use the secure communication channel to send status information to the media playback application, wherein the status information pertains to instructions that were previously received from the media playback application.

15. The system of claim 10, wherein the software component is further configured to use the secure communication channel to receive status requests from the media playback application, and wherein the software component is further configured to use the secure communication channel to send status information to the media playback application, wherein the status information does not pertain to instructions that were previously received from the media playback application.

16. A computing system embodying the system of claim 10.

17. A method comprising:

establishing trust between a media playback application and a downstream component;

establishing a secure channel between the media playback application and the downstream component using a public key associated with the downstream component to encrypt:

a random number provided by the downstream component;

a data integrity key; and

one or more starting numbers;

sending the encrypted data to the downstream component;

using the secure channel to send a command message to the downstream component, the command message comprising a data section that contains a command, and an authentication section that contains data that can be used to authenticate the command;

using the secure channel to request status information from the downstream component; and

using the secure channel to receive a status message from the downstream component, the status message comprising a data section that contains status information, and an authentication section that contains data that can be used to authenticate the status information.

18. The method of claim 17, wherein said one or more starting numbers comprise a starting status sequence number and a starting command sequence number, said numbers being useable to ascertain, respectively, whether a status message or a command message has been lost.

19. The method of claim 17, wherein the act of using the secure channel to request status information from the downstream component comprises sending, with the request, a random number, and wherein the authentication section of the status message comprises data associated with the random number.

20. The method of claim 17, wherein the authentication sections of the command message and the status message comprise data that has been processed using the data integrity key.

21. The method of claim 17, wherein the command message contains a command instructing the downstream component to enable one or more of a number of different types of content protection technologies to protect media content that is provided over a physical connector.

22. The method of claim 17, wherein the downstream component comprises a software driver.

23. One or more computer-readable media having computer-readable instructions which, when executed, implement the method of claim 17.

24. A computing system embodying the one or more computer-readable media of claim 23.

25. The method of claim 17 further comprising using the secure channel to provide protected media content to the downstream component.

26. A system comprising:

one or more computer-readable media;

a software component resident on the media and configured to:

establish trust with a media playback application;

establish a secure channel with the media playback application by providing a public key associated with the software component to the media playback application and receiving back, from the media playback application, encrypted data that has been encrypted with the public key, the encrypted data comprising:

a random number previously provided by the software component;

a data integrity key; and

one or more starting numbers;

use the secure channel to receive a command message from the media playback application, the command message comprising a data section that contains a command, and an authentication section that contains data that can be used to authenticate the command;

use the secure channel to receive status requests from the media playback application; and

use the secure channel to send a status message to the media playback application, the status message comprising a data section that contains status information, and an authentication section that contains data that can be used to authenticate the status information.

27. The system of claim 26, wherein said one or more starting numbers comprise a starting status sequence number and a starting command sequence number, said numbers being useable to ascertain, respectively, whether a status message or a command message has been lost.

28. The system of claim 26, wherein the authentication sections of the command message and the status message comprise data that has been processed using the data integrity key.

29. The system of claim 26, wherein the command message contains a command instructing the software component to enable one or more of a number of different types of content protection technologies to protect media content that is provided over a physical connector.

30. The system of claim 26, wherein the command message contains a command instructing the software component to enable one or more of a number of different types of content protection technologies to protect media content that is provided over a physical connector, and wherein the software component is configured to enable a plurality of different types of content protection technologies.

31. A computing system embodying the system of claim 26.

32. An application program interface (API) embodied on a computer-readable media, the API comprising:

a first method that is callable by a media playback application for establishing trust between the media playback application and a software driver component;

a second method callable by the media playback application for setting up a session key between the media playback application and the software driver component;

a third method that is callable by the media playback application to instruct the software driver component to enable one or more of a number of different types of content protection technologies to protect media content that is provided over a physical connector; and

a fourth method that is callable by the media playback application to request status information from the software driver component.

33. The API of claim 32, wherein the first method receives back a random number generated by the software driver and a digital certificate.

34. The API of claim 32, wherein the second method provides an encrypted concatenation of a random number provided by graphics hardware, one or more session keys, a starting status sequence number, a starting command sequence number.

35. The API of claim 32, wherein the API is exposed by a video rendering component.

36. A method comprising:

calling a device driver to create an instance of a content protection device, individual content protection devices being associated with individual video sessions and serving as an endpoint for communication with a playback application that can send commands and status requests to the content protection devices;

maintaining, with the device driver, a global reference count for each type and level of content protection that is applied to protect content;

maintaining, with at least one content protection device, a local reference count for each type and level of content protection applied through the content protection device; and

adjusting the global and local reference counts in accordance with changing content protection types or levels.

37. A software architecture comprising:

one or more computer-readable media;

software driver code embodied on the computer-readable media and configured to implement multiple content protection devices that are associated with individual video sessions and which serve as an endpoint for communication with a playback application that can send commands and status requests to the content protection devices, wherein the software driver code comprises:

a first method that can be called to determine if a driver supports content protection devices for a given output connector;

a second method that can be called to create an associated content protection device; and

a third method that can be called to determine a length associated with a graphics hardware certificate and to start a video session;

wherein individual content protection devices support callable methods comprising:

a first method to query a graphics hardware certificate length;

a second method to return a variable length graphics hardware digital certificate;

a third method for receiving a concatenation of a data integrity session key, a starting status sequence number and a starting command sequence number all of which are encrypted with a public key associated with the graphics hardware;

a fourth method for receiving a command to change content protection on a physical connector associated with the content protection device; and

a fifth method for querying information about the physical connector being used, the type of protection that can be applied to content being transmitted through the physical connector, and the current protection level that is active on the physical connector.

38. The architecture of claim 37, wherein the content protection device's first method maps directly to the software driver code's third method.

39. The architecture of claim 37, wherein the content protection device's second method maps directly to the software driver code's third method.

40. The architecture of claim 37, wherein the content protection device's third method maps directly to the software driver code's third method.

41. The architecture of claim 37, wherein the content protection device's fourth method maps directly to the software driver code's third method.

42. The architecture of claim 37, wherein the content protection device's fifth method maps directly to the software driver code's third method.

43. A system comprising:

means for establishing a secure communication channel between a media playback application and a component downstream from the media playback application; and

means for using the secure communication channel to at least enable the media playback application to instruct the downstream component to enable one or more of a number of different types of content protection technologies to protect media content that is provided over a physical connector.

44. The system of claim 43, wherein said downstream component comprises a software component.

45. The system of claim 43, wherein said downstream component comprises a hardware component.

46. The system of claim 43, wherein said downstream component comprises a graphics hardware component.